NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

AN ANALYSIS OF DOD FRAUDULENT VENDOR PAYMENTS

by

Shawn R. Jones-Oxendine

September 1999

Principal Advisor: James M. Fremgen

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 1999	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE : AN ANALYSIS OF DOD FRAUDULENT VENDOR PAYMENTS

5. FUNDING NUMBERS

6. AUTHOR(S) Jones-Oxendine, Shawn R.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

Over the last several years, fiscal responsibility in government has been a major issue impacting the Services. As part of fiscal responsibility, the elimination of fraud in the Services is essential. This thesis provides an analysis of fraudulent vendor payments in the DoD. It examines (1) fraud in general, (2) management controls, (3) DoD vendor payment systems, (4) the DoD fraud detection unit, Operation Mongoose, and (5) known DoD fraudulent vendor cases in light of their management control weaknesses. A high risk of fraudulent vendor payments were present in the DoD, pre-DFAS finance and accounting systems and the current DFAS configuration. DFAS has aggressively pursued several initiatives to increase the accuracy of DoD financial management systems and reduce the risks of fraud by using computer technology. The vendor payment cases demonstrate the high risk of fraud due to management control weaknesses. The primary control weakness found include inadequate segregation of duties and unlimited access to the computer systems.

14. SUBJECT TERMS
Fraud, DoD Vendor Payment Systems, Financial Management

15. NUMBER OF PAGES
108

16. PRICE CODE

17. SECURITY CLASSIFI-CATION OF REPORT Unclassified	18. SECURITY CLASSIFI-CATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFI-CATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

Approved for public release; distribution is unlimited.

AN ANALYSIS OF DOD FRAUDULENT VENDOR PAYMENTS

Shawn R. Jones-Oxendine
Lieutenant Commander, United States Navy
B.S., Old Dominion University, 1988

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 1999

Author: ____________________________
Shawn R. Jones-Oxendine

Approved by: ____________________________
James M. Fremgen, Principal Advisor

____
O. Douglas Moses, Associate Advisor

____
Reuben T. Harris, Chairman
Department of Systems Management

ABSTRACT

Over the last several years, fiscal responsibility in government has been a major issue impacting the Services. As part of fiscal responsibility, the elimination of fraud in the Services is essential. This thesis provides an analysis of fraudulent vendor payments in the DoD. It examines (1) fraud in general, (2) management controls, (3) DoD vendor payment systems, (4) the DoD fraud detection unit, Operation Mongoose, and (5) known DoD fraudulent vendor cases in light of their management control weaknesses. A high risk of fraudulent vendor payments were present in the DoD, pre-DFAS finance and accounting systems and the current DFAS configuration. DFAS has aggressively pursued several initiatives to increase the accuracy of DoD financial management systems and reduce the risks of fraud by using computer technology. The vendor payment cases demonstrate the high risk of fraud due to management control weaknesses. The primary control weakness found include inadequate segregation of duties and unlimited access to the computer systems.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

I. INTRODUCTION

A. PURPOSE

The purpose of this thesis is to study misappropriation of Defense Department funds due to fraudulent vendor payments. As of April 1999, of the estimated $11.1 billion dollars in the Department of Defense (DoD) problem disbursements, an estimated $6.8 million is due to misappropriation of Federal funds [Ref. 9]. The objective of this thesis is to conduct an analysis of fraud in general, DoD financial management controls, the vendor payment systems, DoD's fraud detection unit, Operation Mongoose, and known fraudulent cases in DoD.

B. BACKGROUND

Financial management in the DoD has historically been inherently difficult to successfully manage due to its mere size and the billions of transactions that take place on a yearly basis. DoD financial management is the subject of constant criticism, primarily from Congress.

> David Walker, the Comptroller General wrote "Despite DoD's military successes, many DoD programs and operations are still vulnerable to fraud, waste, abuse, and mismanagement, and need improvement". [Ref. 15:p. 3]
>
> In 1998, auditors could not match $22 billion dollars in signed checks with corresponding obligations; $9 billion dollars in known military materials and supplies were unaccounted for; and contractors received $19 million dollars in overpayments. [Ref. 15:p. 4]

This extent of financial mismanagement creates the perfect breeding ground for fraud. Lack of effective management controls is the primary reason fraud can go undetected, particularly fraudulent vendor payments because this type of fraud can easily be committed if proper controls are not in place. The objective of management controls is to make the risk of being caught so high that a would-be thief will decide the risk outweighs the gains. These controls include a reasonable system of checks and balances and segregation of duties in conducting accounting work. They are critical basic guidelines for effective financial management. An effective management control system will decrease the risk of fraud because the system will have "safety" features that make it difficult to commit fraud.

DoD, as well as all other federal agencies, is responsible for ensuring that appropriated funds are used for the purposes and within the amounts authorized by Congress. DoD organizations' accounting systems and funds control systems must be able to accurately record disbursements and expenditures so as to provide reliable information. Since Fiscal Year 1996, DoD is required to submit annual financial statements to Congress. So far, the auditors have issued disclaimers of opinion on the Navy's annual submissions because they could not rely upon the financial information provided. The Navy continues to have problem disbursements, which are defined as payments that have not been matched to corresponding obligations in official accounting records. Problem disbursements are categorized as Unmatched Disbursements (UMDs) or Negative Unliquidated Obligation (NULOs). UMDs occur when an accountable station cannot match a disbursement to a corresponding obligation in the accounting records. NULO's occur when a disbursement report is received, matched to an obligation, and posted to the appropriations by the accountable station, but the recorded disbursement exceeds the recorded obligation. Another category is in-transit disbursements. In-transit disbursements refer to disbursements and collections that have been reported to the Treasury but have either not been received by the accounting station or have been received but not processed or posted by the accounting station. For the in-transit category, DFAS reports as problem disbursements transactions it considers over-aged--specifically those (1) over 60 days old if the disbursing and accounting stations are assigned the same DFAS center or (2) over 120 days old if the disbursing station is assigned to one DFAS center and the accounting station is assigned to another DFAS center, DoD component, or federal agency. These problem disbursements are key to the analysis of fraudulent vendor payments.

Due to the government drawdown since 1991 and the attempt to become fiscally responsible, the DoD financial management system has changed dramatically. One change is the regional consolidation of the Defense Finance and Accounting Service (DFAS) Operation Locations (OPLOCs). For example, the

Navy went from 15 finance centers in Fiscal Year (FY) 1993 to 6 OPLOCs and a DFAS headquarters in Cleveland Ohio [Ref. 2:Module D-23]. These OPLOCs and those of the other Services are DoD's bill payers and are the primary locations where fraudulent payments are likely to occur.

To enhance the DoD fraud detection capability, Operation Mongoose was created in 1994 with the primary purpose of detecting fraud in retired and annuitant pay, military pay, civilian pay, transportation payments, and vendor payments. This thesis reviews the impact of Operation Mongoose on fraudulent vendor payments in DoD and the Services.

C. RESEARCH QUESTIONS

1. Primary Questions

The primary research question this thesis will attempt to answer is as follows: How has the consolidation/organization of the vendor payment system impacted the detection and prevention of fraudulent vendor payments?

2. Secondary Questions

a. How has computer technology impacted the detection and prevention of fraudulent vendor payments?

b. How effective are financial management instructions/controls in detecting fraudulent vendor payment?

c. What, if any, are the geographical, technological, or biographical trends in fraud cases already uncovered in DoD?

D. SCOPE OF THESIS

The scope includes the following stages regarding fraudulent vendor payments: an overview of fraud in the DoD, (2) management controls and the DoD vendor payment systems, (3) an in-depth review of current vendor payment systems and the risks of fraudulent vendor payments, (4) computer technology and the risks of fraudulent vendor payments, (5) a review of the DoD fraud detection unit, Operation Mongoose, and (6) an analysis of fraud cases.

E. METHODOLOGY

The methodology used in this study of fraud consists of the following steps:

- Conduct a literature research of financial management regulations, Government Accounting Office (GAO) reports, Navy Audit reports, books, library resources, and Internet resources.

- Conduct an in-depth review of fraudulent vendor payments in the Services with emphasis on the Navy.

- Examine the consolidation of the vendor payment systems.

- Conduct an extensive review of the fraud detection methods of Operation Mongoose. Conduct site visits to Operation Mongoose, Seaside, CA.

- Collect and analyze data in fraud cases in light of management controls.

- Prepare an assessment of the DoD's prevention and detection of fraudulent vendor payments.

F. ORGANIZATION

Chapter II provides an overview of fraud in general. It describes types of fraud and characteristics of a possible fraud perpetrator. It provides an historical view of fraud awareness in the federal government. Chapter II provides information on the current issues involving fraud in the federal government and the DoD. The chapter concludes with the legislative initiatives which spearheaded the focus on financial management practices in DoD.

Chapter III introduces management controls in DoD finance and accounting. It discusses the factors that influence the integrity of organizations financial and accounting methods. It reviews the general and specific controls set forth in Office of Management and Budget (OMB) Circular A-123 and risk management in the DoD.

Chapter IV discusses the DoD vendor payment systems and the risks of fraudulent vendor payments. It gives an overview of the past and present organizational structure of the DoD's bill paying system. The chapter concludes with current initiatives for improving the bill paying system.

Chapter V discusses the DoD fraud detection unit, Operation Mongoose. It reviews its mission, operational systems, and prevention and detection methods. It concludes with an evaluation of fraud detection results produced by Operation Mongoose.

Chapter VI reviews cases involving fraudulent vendor payments in the DoD in light of management control weaknesses that allowed the frauds to occur.

Chapter VII summarizes findings of the research, answers the research questions, interprets the data from the case analysis, and presents recommendations for further research and study.

G. EXPECTED BENEFITS OF THIS THESIS

Over the last several years, fiscal responsibility in the government has been a major issue impacting the Services. As part of fiscal responsibility, the elimination of fraud in the Services is essential. An analysis of fraudulent vendor payments gives an assessment of where the Services are in preventing and detecting fraud. This thesis may be used as a quick reference for the financial manager who desires an overview of vendor fraud and all the relevant issues surrounding it.

THIS PAGE INTENTIONALLY LEFT BLANK

II. OVERVIEW OF FRAUD

A. FRAUD DEFINED

Fraud in the Federal Government can be described in many forms. Mckinney and Johnson state that fraud involves dishonesty, illegality, and the intentional wrongful obtaining of either money or benefits [Ref. 11:p. 5]. It includes theft, embezzlement, false statements, illegal commissions, deceit by suppression of the truth, kickbacks, conspiracies, obtaining contracts through collusive arrangements, and the intentional mischarging or misallocation of contract costs. The Association of Certified Fraud Examiners (ACFE) states that fraud occurs when, for personal gain, employees put forth some type of deception [Ref. 4:p. 1]. They place fraud into three major categories: (1) corruption which includes bribery, extortion, and conflict of interest, etc., (2) asset misappropriation, which includes ghost employees, shell companies, forgery, etc., and (3) fraudulent financial statements. The ACFE in a recent report on fraud has determined that asset misappropriation accounts for more than four out of five fraud offenses [Ref. 4:p. 3]. Below are two primary means of fund misappropriation.

1. Shell Companies

Shell companies normally involve phony companies to which vendor payments are made for products or services. These nonexistent companies are set up to receive misappropriated funds, which are then used by the perpetrator. Fraudulent invoices and receiving reports of goods are normally used to create the false liability. The funds may be transferred to accounts electronically, forwarded to post office boxes, or sent to "front" address.

2. Ghost Employees

Ghost employees, also called fictitious employees, is a category of fraud which involves the fraudulent payment of money to phony employees or others. In many cases, bogus eligibility data is drawn from identifying deceased or living persons who are not eligible or entitled to the payments. With respect to DoD, a perpetrator may create accounts for active duty or retired persons and deposit funds in these accounts for his or her personal use. In some instances the perpetrator may send the fraudulent payments to relatives, friends, or other accomplices.

B. FRAUD INDICATORS

The ACFE conducted a comprehensive study, which began in 1993, in which it collected fraud case data from 2,608 Certified Fraud Examiners.

> One thousand four hundred and ninety eight of these cases began after 1985. Fraud and abuse cases totaling $15 billion over the last 10 years are covered in the report. The data was collected from 12 major industry groups including the federal government. [Ref. 4:p.1]

This study showed that there are certain patterns in the characteristics of employees who commit fraud. Two primary indicators were position in the organization and lifestyle changes.

1. Position in Organization

The data indicated that about 58 percent of the reported fraud and abuse cases were committed by nonmanagerial employees, 30 percent by managers, and 12 percent by owners/executives.

2. Lifestyle

The lifestyle of an employee is a possible indicator of fraud. If an employee with access to accounting records has affected a change in lifestyle that seems out of proportion to his or her paycheck (i.e., an expensive new car, lavish vacation, expensive recreational property, outside investments, etc.), he or she may be committing fraud. These types of observations are highly subjective and judgmental and care should be taken to avoid impropriety [Ref. 5:p. 1]. Also, an employee who is extremely hesitant or refuses to take regular annual vacation days off could be one who needs to be present to sustain a misappropriation scheme. The perpetrator does not want anyone to fill in, out of fear of being discovered.

C. FRAUD ENVIRONMENT

Combinations of factors influence the fraud environment. The primary conditions are motivation, personal integrity, and opportunity. These factors will interact to determine whether a person will commit fraud.

1. Motivation

The motivation to commit fraud against the government may stem from a variety of reasons. Personal debts and losses, living beyond one's means, and greed are some possible factors. Other reasons may include resentment of superiors, perceived inequalities, gambling, or urgent need for favorable performance [Ref. 9]. An example of urgent need for favorable performance is altering disbursement document data to make payment dates appear on time and avoid interest charges. One case in Chapter VI involves this type of action.

2. Personal Integrity

Individuals lacking honesty may or may not behave correctly, depending on the situation. Management can insist on high standards of integrity and reinforce those standards by their own conduct, thereby setting a moral tone that does much to influence thought and conduct throughout the organization [Ref. 6].

3. Opportunity

Naturally, managers trust employees and believe operations are well-managed and under control. However, this mentality creates a perfect environment for fraud.

> One survey found that managers place too much trust in employees, lack procedures for authorization, lack separation of duties, conduct no independent check on performance, lack adequate attention to detail, and had sloppy procedures. [Ref. 10:p. 74]

D. HISTORICAL PERSPECTIVE OF FRAUD IN THE DOD

In 1973, the University of Michigan Institute for Social Research reported a sharp drop of American trust in government [Ref. 11:p. 2]. Many felt that tax money was wasted and misappropriated. In another study completed in 1980, the percentage saying they always trust government fell below 30 percent [Ref. 11:p. 2]. Much of the lack of trust stemmed from the stories of the Pentagon's $1000 ladders and $600 toilet seats.

While a few isolated studies of fraud were commissioned by the federal government in response to negative publicity, it was not until the end of the 1970's that a systematic analysis began to take place. By the end of 1979, a federal anti-fraud movement had begun [Ref. 11:p. 60]. Congress passed the Inspector General Act, creating top level posts in each executive agency for the coordination of audit and investigative resources. The Act also requires annual reports from each inspector general to Congress. In 1979-80, the GAO launched it's "Fraud Hotline" [Ref. 11]. Although the hotline worked well within DoD overall, in 1983 the Navy issued supplemental guidelines for handling Inspector General (IG) complaints. The Navy found three major deficiencies in it's fraud hotline: (1) the investigators were not objective, (2) the files lacked relevant and competent documentary evidence, and (3) investigations were conducted with minimal information on work done. The Navy believed the hotlines were an important tool in preventing fraud, waste, and abuse. At that point in 1983, 27 percent of the reports were substantiated and resulted in $5.3 million in savings [Ref. 12].

Also in 1980, the Office of Management and Budget (OMB) issued a directive to all agencies calling for the assessment of all aspects of program administrative operations for potential areas of fraud and abuse. Congress enacted legislation which requires continuing evaluation of internal accounting and administrative control systems in each agency. President Reagan's Grace Commission mounted a comprehensive study of federal spending in many areas of the government. Toward the end of President Reagan's first term, the Commission submitted proposals which, it claimed, could save the federal government more than $400 billion over three years [Ref. 11:p. 61].

E. CURRENT FRAUD ISSUES IN DOD

Since the early 1990's, Congress and the DoD have made serious attempts to impart integrity in the financial management system, especially the elimination of embarrassing fraud and waste. The DoD accounting systems have undergone numerous changes in an effort to establish more controls, reduce redundancy, reduce paperwork, and increase reliability of financial information.

In order to assist in combating fraud, many federal agencies have combined forces to form task groups and/or share information. For example, Operation Mongoose, the DoD fraud detection unit, has formed an alliance with the DoD

Inspector General (DoD, IG), the United States Secret Service, and Service audit agencies. The Defense Finance and Accounting Service (DFAS) established a partnership with the Defense Criminal Investigative Service (DCIS) and the Air Force Audit Agency. In February 1998, DFAS also created a Fraud Task Force. The DFAS director, Leon Krushinski, states in a recent Navy Comptroller article:

> Fraud detection and prevention are critical concerns for all of us, with today's declining resources in DoD, we must work together to strengthen our operations and stop fraud. [Ref. 14:p. 3]

The current culture in DoD is to launch an aggressive campaign to eliminate fraud. There are two key areas relating to the elimination of fraud. They are the financial statements, which all Services must submit, and problem disbursements in the financial management system.

1. Financial Statements

Since FY 1996, the Services are required to submit audited financial statements to Congress. The Navy has received a disclaimer of opinion on its fiscal year 1996, 1997, and 1998 financial statements. The auditors were unable to render an opinion due primarily to the unreliable information as to the value of its assets, liabilities, and status of funds [Ref. 14:p. 16]. Auditors also reported that DoD's long-standing weaknesses in its financial management operations undermine its ability to manage an estimated $1 trillion in assets and limit the reliability of financial information provided to Congress [Ref. 25:p. 13]. The elimination of fraud will increase the accuracy of DoD's financial statements.

1. Problem Disbursements

Problem disbursements are specific disbursements that have not been matched with a corresponding obligation. These disbursements increase the risk of fraudulent or erroneous payments being made without detection. The cumulative amounts of these disbursements may exceed appropriated amounts and other legal limits. Of the $11.1 billion dollars in UMDs and NULOs in 1998, $5.7 billion (51%) was in the Navy [Ref. 1:p. 11]. Since FY 1990, DFAS has worked on many initiatives aimed at reducing or eliminating problem disbursements. Primary emphasis has been on changing existing business processes to speed up the posting of disbursements and collections to accounting systems and to improve the accuracy of disbursing and accounting information. Six of the major initiatives to reduce problem disbursements include Centralized Disbursing, Defense Cash Accountability System, Defense Procurement Payment System, On-line Payment and Collection, Prevalidation, and Transaction For Other Cell. These improvements will be discussed further in Chapter IV. The following Figure 1 below shows the trends in DoD problem disbursements:

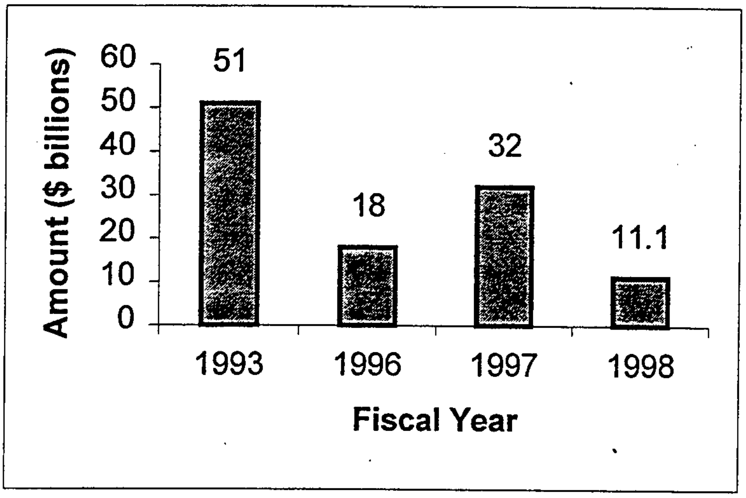

Figure 1. Trends in DoD Problem Disbursements [Ref. 1]

F. LEGISLATIVE INITIATIVES

Behind the push to eliminate fraud in the DoD are four significant legislative acts that directly impact the financial management systems in the DoD. These acts include the Federal Managers' Financial Integrity Act of 1982, the Chief Financial Officers Act of 1990, the Government Management Reform Act of 1994, and the Federal Financial Management Improvement Act of 1996. In fraudulent vendor cases, although transactions may be recorded they are not legitimate entries. This false information distorts any attempt to accurately reflect assets and liabilities, demonstrates lack of internal controls, and reflects a weak accounting system. Thus, it violates each of these relevant laws.

1. The Federal Managers' Financial Integrity Act (FMFIA) of 1982 [Ref. 40]

This Act requires that federal agencies ensure that obligations and costs comply with applicable law. In addition, it requires that revenues and expenditures that apply to agency operations are recorded and accounted for properly so that accounts and reliable financial and statistical reports may be prepared and accountability of assets may be maintained. The Act primarily focuses on internal accounting and administrative control in order to safeguard funds, property, and other assets against waste, loss, unauthorized use, and misappropriation.

2. The Chief Financial Officers Act (CFO) of 1990 [Ref. 41]

Congress passed the CFO Act so that federal agencies may provide improved systems of accounting, financial management, and internal controls. The key directives require that each agency prepares financial statements for its operations and have them audited.

3. Government Management Reform Act (GMRA) of 1994 [Ref. 41]

The primary reason for this act was to add more detailed requirements to the CFO Act. It was designed promote more effective and efficient financial management. This Act directs agencies to streamline management controls and enforce electronic payments, and it offers more guidance on the submission of financial statements.

4. The Federal Financial Management Improvement Act (FFMIA) of 1996 [Ref. 41]

The FFMIA Act of 1996 requires auditors to perform financial audits to determine whether agencies' financial management systems comply substantially with Federal Accounting Standards, financial system requirements, and the government's standard ledger at the transaction level.

G. CHAPTER SUMMARY

Fraud in the DoD is basically defined in three major categories and misappropriation is the largest category causing the largest monetary losses in DoD. The possibility of fraud is high if the right combination of opportunity, motivation, and level of personal integrity occurs. Historically, fraud in DoD did not receive much attention. Action was taken seriously only when occasional isolated cases became highly publicized. The DoD has historically had weak internal controls and a lack of financial accountability, which are primary facilitators of fraud. Recent major legislative initiatives and the declining resources of DoD have spearheaded the movement to eliminate fraud and waste.

III. MANAGEMENT CONTROLS

A. DEFINITION

> Internal controls consist of any and all procedures and policies established to ensure that what goes on inside an organization is done right. Internal controls are designed to ensure that operations are conducted effectively, efficiently, and in compliance with the law and that information recorded and reported is reliable. [Ref. 28:p. 1]

With a good system of internal controls, managers can set standards with which to judge organizational effectiveness, allowing weaknesses to be detected and corrected. The policy of the DoD is that internal controls are management's responsibility and should be in effect across the board in every organization within each DoD component. Although internal controls in themselves cannot prevent every incident of waste, mismanagement and fraud, DoD policy is to ensure that resources are properly managed and controlled.

B. TYPES OF CONTROLS

Government controls are classified as general or specific. These controls are a requirement of FMFIA and are prescribed in OMB Circular A-123 [Ref. 7]. General standards for control are noted below:

1. Compliance With Law

All program operations, obligations, and costs must comply with applicable law and regulation. Resources should be effectively and efficiently allocated for duly authorized purposes.

2. Reasonable Assurance and Safeguards

Management controls must provide reasonable assurance that assets are safeguarded against waste, loss, unauthorized use, and misappropriation. The management controls developed for each agency should be logical, applicable, reasonably complete, and effective and efficient in accomplishing objectives.

3. Integrity, Competence, and Attitude

Managers and employees must have personal integrity and are obligated to support any ethics program in their agencies. The spirit of the Standards of Ethical Conduct [Ref. 8] requires that employees develop and implement effective management controls and maintain a level of competence that allows them to accomplish their assignments. Also, effective communication within and between offices should be encouraged.

The specific management controls relate directly to the processes involved in vendor payments and are where most weakness occur. Specific standards will be discussed in detail due to their significant relevance to fraudulent vendor payments. The specific controls are as follows:

4. Delegation of Authority and Organization

Managers should ensure that appropriate authority, responsibility and accountability are defined and delegated to accomplish the mission of the organization, and that an appropriate structure is established to effectively carry out program responsibilities. Controls and related decision-making authority should be the responsibility of line managers and staff to the fullest extent possible.

5. Separation of Duties

Key duties and responsibilities in authorizing, processing, recording, and reviewing agency transactions should be separated among individuals. Managers should exercise appropriate oversight to ensure individuals do not exceed or abuse their assigned duties.

> Probably no other control activity has received more attention than the proper segregation of duties among independent parties. No one person should be responsible for all aspects of a transaction.... If such a situation were allowed, that person might make errors that no one else would detect. Worse, he or she might commit fraud and cover all traces of it. Specifically, no one person should have responsibility for (1) authorizing a transaction, (2) access to related assets, and (3) accounting for the transaction. For example, if one person could authorize a cash payment (e. g., approve the payment of a bill), prepare and sign the check...and record the payment, he could approve a fictitious bill, write a check for himself or a dummy organization... and record the payment as though it were a valid purchase of goods or services.
>
> Segregation of duties builds a cross-check on the activities of each individual into the system. It also reduces the opportunity and thus, the incentive to commit fraud.
>
> In a computerized system, the functions of system design, programming, and computer operation, data entry, and maintenance of programs and data files should be kept separate. [Ref. 28:pp. 16-17]

One problem with segregation of duties controls is the possibility of collusion. Collusion is defined as an agreement between two or more persons to defraud organizations or persons of their property, or to obtain an object forbidden by law [Ref. 41]. Many of the best internal control procedures depend for their effectiveness on some segregation of responsibility. Such controls are vulnerable to collusion between the employees charged with the separate responsibilities. Collusion can also involve an employee acting with an outsider, such as a customer, vendor or supplier.

Collusion among employees and vendors, when it happens is difficult to detect. Supervisory oversight and monitoring is key in preventing collusion but it may not be enough. This is why limited access to accounting systems, and authority to certify invoices and approve disbursements is critical.

6. Access to and Accountability for Resources

Access to resources and records should be limited to authorized individuals, and accountability for the custody and use of resources should be assigned and maintained. Access to invoices, databases, and payment vouchers must be strictly controlled. In a computer based payment system, access to vendor payment systems and the ability to manipulate data in the payment systems must be controlled, delegated, and monitored in order to prevent fraud, errors, and the overall integrity of the systems.

7. Recording and Documentation

Internal control systems and all transactions and other significant events are to be clearly documented and the documentation is to be readily available for examination. If documents are prepared faithfully and accurately, the data entering the system should be reliable and complete [Ref. 28:p. 18]. The document should be designed to fit the specific features of each transaction. Data entered into a computer can be identified and stored as a unique transaction. In the vendor payment systems, management should regularly review and compare disbursements, invoices, receiving reports, and vouchers in order to determine if any discrepancies exist. If discrepancies are found, they should immediately be investigated.

a. Pre-numbering and Sequential Use

In the vendor payment systems the important documents are the purchase requisition, purchase order, and receiving report. An important feature of documents is that they should be prenumbered and used in numerical sequence. If documents are not pre-numbered and used in sequence, they might be lost or concealed and transactions, never recorded [Ref. 28:p. 19]. In a computerized vendor pay system these features should automatically be incorporated.

b. Standardized Procedures/Data Entry

Standardized procedures and data entry enables management to detect errors and non-compliance. In a computerized system, standardized data allows easier transaction analysis, tracing, and verification. It also decreases the chances of someone intentionally altering data to create discrepancies, for example, intentionally altering a vendor's address in order to create shell companies and divert funds.

c. *Information Processing*

The reliability of financial information depends on controls over the data that enters the accounting system. These controls should focus on the information processing systems themselves (e. g., restrictions on access to computers and data files) and also on the processing of specific transactions [Ref. 28:p. 16]. In the vendor payment system the ability to delete, add, alter, and create documents must be tightly controlled, especially in computerized systems. No one individual should control all key aspects of a transaction or event without appropriate controls.

8. Adequate Supervision

Qualified and continuous supervision is to be provided to ensure that internal control objectives are achieved and approved procedures are followed. Managers at all levels should be sensitive to indications that internal controls are not working as they should [Ref. 28:p. 19].

9. Resolution of Audit Findings and other Deficiencies

Managers should promptly evaluate and determine proper actions in response to known deficiencies, reported audit and other findings, and related recommendations. Managers should complete all action items within the prescribed timeframe.

C. RISK ASSESSMENT

In the DoD finance and accounting systems, financial managers must regularly assess all of their operations and procedures to determine the existence of risks and the consequent risk of failures of internal controls. Since there are so many rapid changes to improve the vendor payment systems in the DoD, it is imperative that management ensure that with the consolidations, improved systems, and use of computer technology, they ensure proper controls are in place to significantly reduce the risks that fraudulent vendor payments can be made.

> The DoD agencies must implement a careful balance of controls. Too much control stifles initiative, produces redundant controls, and can be labor intensive. Conversely, too little control leads to inefficient use of resources, violations of statutes, and an increased opportunity for fraud. [Ref. 1]

In the past, DoD agencies were required to submit a vulnerability assessment which identified areas that were considered high risk regarding fraud, theft, inefficiencies, etc. This assessment is no longer required, however. Under the FMFIA, agencies are required to report to Congress an annual statement of assurance which reports accomplishments, material weaknesses, and actions taken and planned to correct the weaknesses.

The GAO standards strongly suggest a Senior Management Council. GAO considers the Senior Management Council the most important unit of internal control [Ref. 29]. The primary purposes of the Council are to question top management, see that corrective actions are taken when weaknesses are discovered, and keep management from overriding internal control.

IV. VENDOR PAYMENT SYSTEMS

A. INTRODUCTION

Since fraudulent vendor payments normally occur at the point where these payments are made, it is important to understand the DoD bill paying process. The DoD's bill paying process has undergone major changes since the 1980's. Major reorganizations have occurred that may have impacted the presence of fraudulent vendor payments. This chapter provides an analysis of the DoD vendor payment systems with some detailed information on the Navy's systems.

B. INTRODUCTION TO NAVY ACCOUNTING

The Navy maintains a formalized system called the Resource Management System (RMS) by which it tracks and accounts for financial resources provided to and employed by Navy shore commands within the Operations and Maintenance (O&MN) appropriation. Before 1968 and the implementation of RMS, funding for field activities was provided in numerous allotments for specific areas or items. This type of funding placed very specific limits on the resources made available to commanding officers and somewhat restricted the commanding officer's ability to carry out the mission. The implementation of consolidated funding under RMS allowed commanding officers to remove the financial boundaries and gave them more freedom to carry out their missions.

The accounting system developed for RMS provides accounts, records, and procedures for recording financial transactions. It was designed to include accounting and budgeting controls. The system requires the same actions that are used in accounting in the commercial sector, i.e., recording, classifying, summarizing (reporting), and interpreting the effect of all financial transactions. The accounts and records are designed to provide cost and management information required by commanding officers and department heads, cost center managers, the fleet command, type command, system command, office bureau, the Office of Comptroller of the Navy, the Office of the Secretary of Defense, and the Office of Management and Budget.

1. General Funds

General funds accounting is used to record money appropriated by Congress and the financial transactions using the funds. The Navy manages 24 general fund accounts. These accounts are funded by either current year appropriations, multi-year appropriations, or no year appropriations (appropriations that are available for incurring obligations until exhausted or until the purpose for which the funds were made available has been accomplished).

2. The Accounting Transaction Cycle

Although defense accounting and finance offices use numerous automated systems to process vendor payments, the basic steps to initializing a transaction in the vendor payment systems are similar. The following are steps that begin the accounting transaction:

- A request form is prepared to place an order for an item. The request form could be a requisition or any other local purchasing document that identifies the activity requesting the item, a description of the item, and its estimated cost.

- When a request is prepared, accounting data is assigned to the order in the form of a document number and a job order number for cost accounting purposes.. The request is then recorded in the cost center's local memorandum records (e.g., OPTAR log) with a copy being forwarded to the comptroller, who will establish an obligation in the official accounting system.

- The original request is passed to the purchasing authority for action. The document number, job order number (JON) and estimated cost are important because they are recorded in the cost center's unofficial or memorandum records to establish an obligation. An obligation must be entered in the memorandum records immediately to reserve funds for future payment and track the current balance.

- At a later date, the activity receives the item from the supplier along with an invoice. The activity ensures all purchase requirements are met (i.e., quantity, condition, item) and certifies the invoice for payment.

- The certified invoice is forwarded to the paying office for payment. Though the item has been received, it still remains an obligation in the activity memorandum records and will not be recorded as an expenditure until the paying office pays the bill and records the expenditure.

- The paying office audits the invoice against the copy of the purchase document (forwarded with the certified invoice) and makes sure there is an obligation on file.

- A check is mailed or funds are electronically transferred to the vendor and an expenditure is recorded in the official records.

- Using the Financial Reporting System (FRS) expenditure data is forwarded by the paying office to the DFAS Center OPLOC for reporting to the activity's responsible/administering office and to the Treasury. If the expenditures cannot be matched with obligations already established in the official records, it will error out to the Unmatched Funds Disbursed Suspense File (problem disbursements). They will remain in suspense until they are reconciled with a matching obligation. [Ref. 1]

C. CURRENT NAVY VENDOR PAYMENT SYSTEM

1. Standard Accounting and Reporting System-Field Level (STARS-FL)

The Navy currently uses two separate vendor/contract payment systems, STARS-FL and Mechanization of Contract Administration Services (MOCAS). Vendor payments normally are categorized as small, local purchases with dollar amounts generally less than $25,000, although higher amounts are disbursed depending on the items purchased. The primary system for vendor payments is STARS-FL, which provides general fund accounting and bill paying support to the Navy. STARS-FL manages about $750 billion in present and past year funds [Ref. 19: Sec 2]. It will support over 1,000 activities and 15,000 users worldwide. STARS-FL is composed of four major subsystems: Field Level Accounting; Headquarters Accounting and Reporting for funds administrators, major claimants and systems commands; One Bill Pay; and Funds Distribution and Departmental Reporting. STARS-FL is a DFAS owned system and is supported by the Navy's

Fleet Material Support Office Central Design Activity. The STARS-FL bill paying process is depicted in Figure 4.1.

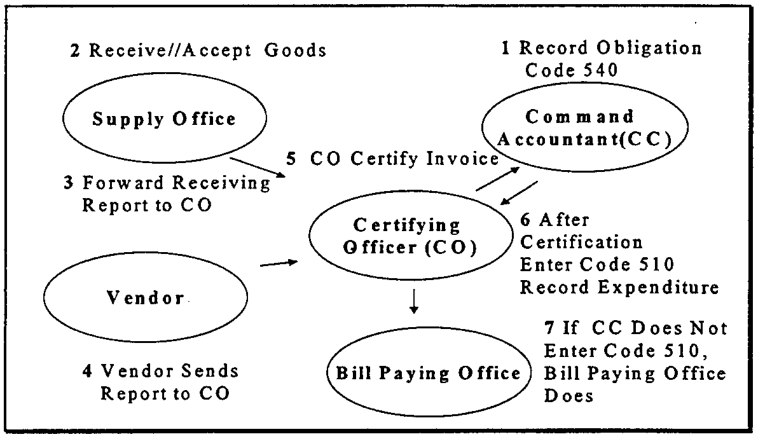
2 Receive//Accept Goods
1 Record Obligation Code 540
Supply Office
Command Accountant(CC)
5 CO Certify Invoice
3 Forward Receiving Report to CO
Certifying Officer (CO)
6 After Certification Enter Code 510 Record Expenditure
Vendor
7 If CC Does Not Enter Code 510, Bill Paying Office Does
4 Vendor Sends Report to CO
Bill Paying Office

Figure 4.1. STARS-FL Vendor Payment System [Ref. 30]

a. Uniform General Ledger Account (UGLA)

The Navy uses the UGLA to record general ledger information in the STARS-FL. The UGLA is not a transaction-driven standard general accounting system capable of accurately reporting the value of assets and liabilities, including the status of appropriated funds as required by law. The UGLA also does not have subsidiary ledgers, which are necessary for maintaining accurate financial records and providing audit trails. This data is needed for financial reporting as required by the CFO Act, OMB, and DoD. The UGLA provides for seven classifications of accounts. The vendor payments fall under the liability accounts classification. The STARS-FL system, using the UGLA, is comparable to cash basis accounting in that payables are not recognized until final stages of the bill paying process (receipt of invoice or at the time of disbursement). The DoD is required to implement accrual accounting, which recognizes a payable upon receipt of goods or services. Accrual accounting provides a more realistic picture of payables and receivables.

b. The Switch to Standard General Ledger (SGL)

The general ledger is the book of accounts in which all accounting entries are ultimately summarized. The general ledger account structure is specifically designed for accrual accounting and is in compliance with the law. SGL also provides more specific detailed categories to better summarize and classify for accurate financial reporting. Beginning in FY 1996, the Navy began the transition from UGLA to SGL, as required by law. To date, the Navy has not fully implemented SGL. It is still unable to use accrual accounting, as noted on its audited financial statements from FY 1996, 1997, and 1998 [Ref. 14].

2. Mechanization of Contract Administration Services (MOCAS)

The MOCAS is the primary DoD contract entitlement and payment system used by the DFAS Columbus, Center. MOCAS pays over 400,000 contracts per year [Ref. 29:p. D-55]. The MOCAS system does not normally include vendor payments. Contract payments include large dollar amounts, normally over $25,000, and require special administration. However, the process of payment and problems associated with this system are similar to the vendor payment system.

3. Other Navy Vendor Payment Systems

The Navy also uses the following systems to a lesser degree: Facilities Information System which is used by Naval Facilities Engineering Command accounting entities, the IDAFMS, the Navy Industrial Fund Management System, Financial Management Information System, Integrated Financial Management System, Naval Ordnance Management Information System, Naval Ocean System Center Finance and Accounting System, Navy Military Transportation Office Automated Transportation Data System, and Shipyard Management Information System defense finance and accounting services.

4. DFAS Feeder Systems

Approximately 80 percent of the DoD financial data are derived from program feeder systems. They are called feeder systems because they provide data to the financial systems. Program feeder systems are automated or manual systems operated by the Military Departments and the Defense Agencies. The STARS-FL located at Navy commands and DFAS accounting stations "feed" vendor payment data to DFAS OPLOCs for payment. These systems contain day-to-day operating information that needs to be translated into useful financial information for financial managers. These feeder systems are not under adequate general ledger control and do not comply with federal requirements [Ref. 20:p. iii]. DFAS is making efforts to bring these feeder systems into compliance with applicable federal requirements. Figure 4.2 below shows the feeder systems reduction efforts.

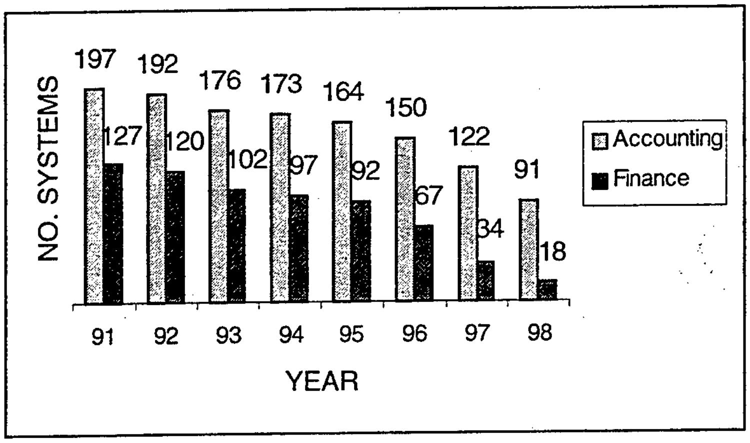

Figure 4.2. Feeder System Reductions [Ref. 19]

So many systems exist in DoD because there was no directive or reason for having standardized systems in the past. The massive paperflow and the incompatibility of the systems contributed to the accumulation of problem disbursements. The transmittal of critical financial data for vendor payments was often incomplete. Incomplete and inaccurate vendor payment databases hindered the process of prevalidating vendor payments, detecting erroneous, duplicate, and fraudulent payments. Since FY 1990, DFAS has reported to the DoD, IG, that lack of effective interface between payment systems and accounting systems as a material weakness [Ref. 1:p. i].

D. DFAS PRE-CONSOLIDATION AND FRAUDULENT PAYMENT RISKS

Since 1947, the DoD has had a decentralized mode of operations. The three military departments and other DoD agencies have, until recent reforms began, always managed their own budget, finance, and accounting systems. They developed distinct processes and business practices, geared to their particular missions and with little need to achieve compatibility with other DoD operations. The financial management organizations of each of the Services combined (DFAS not established yet) had 250 financial accounting systems and 332 field offices (former AAAs). These offices were scattered throughout the United States and Overseas.

This DFAS pre-consolidation period had numerous problems which increased the risk of fraudulent payments. Below are ten prominent problems associated with the vendor payment processes found by the DoD, IG [Ref. 18:p. 23]. These problems are representative of the typical finance and accounting offices throughout the Pre-DFAS organization.

1. Non-Standard Data

Names, addresses, and other data fields used to test data validity were not standardized. Accounting technicians used many different formats (i.e., Street and ST, road and rd, incorporated and inc.). This type of non-standardization poses a high risk of fraudulent payments, because someone can intentionally duplicate a vendor address or name with slight differences when submitting data for payment. These funds can be diverted to fictitious vendor accounts.

2. Edit Checks

Some software did not contain adequate edit checks to ensure the data were reliable. Edit checks are needed to ensure that each contract number is unique and does not appear in more than one vendor payment data base, that each payment address meets a standard format, and that each payment number is unique. Because these controls were not in place, an excessive amount of transactions were identified as potentially fraudulent payments [Ref. 23:p. 8].

3. System Incompatibility

Two vendor payment systems did not validate the transfer between each other for dollar amounts and transaction totals. Without this validation, data could be changed, added, or deleted when transferred between systems without being detected.

4. Operating Procedures

Operational procedures were inadequate or not being followed by accounting technicians. Payments were sent to vendors with addresses shown on the invoice that differed from the addresses shown on the contracts. Financial Management Regulations specifically state that the name and address of the vendor official to whom payment is to be sent must be the same as that in the contract or in proper notice of assignment.

5. Sign-Out Procedures

Controls over file management were weak because personnel did not follow sign-out procedures. Personnel could not locate 110 (15 percent) of 750 contract payment files that were requested because technicians did not follow established sign-out procedures. Personnel were required to sign out the file folders when removing them from storage. Auditors noted that the technicians emphasized the need to file contract folders properly, but gave priority to processing payments [Ref. 23:p. 9]. The risk of making erroneous or fraudulent payments increase if, in a rush to process payments, contract files are not checked for legitimacy.

6. Lack of Effective Routines

> One computer routine identified 123 payments that had duplicate contract numbers and payment numbers in one vendor payment database. This routine accounted for $161,824 of the $208,404 in actual and potential duplicate payments and overpayments. [Ref. 23:p. 9]

These payments were made because the accounting technicians were not required to research the history files to determine whether payments had already been made. If the technician could not locate the original hard copy file, a dummy contract payment file was created. Payments were also made on duplicate invoices.

7. Control Over Access to Vendor Payment Data

The local area network (LAN) software used to communicate with the vendor payment data lacked adequate controls. The LAN system allowed users to perform specific actions: read, write, create, erase, modify, and scan. Supervisors did not periodically review access to the vendor payment systems. The security officer did not send reports on assigned users to supervisors to ensure that user access was removed when no longer needed. In addition, automated records were not properly safeguarded from compromise.

8. Control Over Access to Local Area Network (LAN)

The security officer did not provide key reports to supervisors so that they could properly control access to the LAN.

> Out of 1,110 users, 681 (61 percent) did not have passwords. Also, 186 (43 percent) of the 429 users with passwords had not accessed the system during the previous 3 weeks or more. When the LAN was installed, users were given access regardless of need. [Ref. 23:p. 15]

9. Misuse of SuperQuery

Management did not have an adequate trail for changes and deletions to the primary vendor pay systems. Fifty-five employees had access to SuperQuery, a software utility program that allows a user to update, insert, and erase data sets without leaving an audit trail in the database [Ref. 23:p. 15]. Audit trails are critical in protecting against fraudulent vendor payments.

10. Lost Vendor Payment Data Prior to Consolidation

During the consolidation phase some accounting stations were closing and others remained open and took on the work of the closing offices. Much of the financial information was lost during the transfer because procedures for transferring and tracking records and data did not exist. In April 1993, approximately 200 open contracts from one closing office were lost and could not be audited to validate vendor payments [Ref. 18:p. 13]. Also, data tapes with vendor data from a closing accounting office were erased by personnel at one accounting office because they were not picked up by the gaining office. As a result of vast amount of historical data being lost during transfer, DFAS developed and distributed a checklist covering consolidation procedures. Again, the risks of erroneous payments and fraudulent payments are high because the required documentation (invoices, contract, receiving reports) cannot be compared to disbursement data.

These major problems substantially increased the risk of fraudulent payments and contributed to the decision to consolidate the functions and form the current DFAS configuration.

E. CURRENT DFAS AND FRAUDULENT VENDOR PAYMENT RISKS

DFAS was activated in January 1991 to reduce the cost and improve the overall quality of DoD financial management through consolidation, standardization and integration of finance and accounting operations, procedures, and systems. Also contributing to the decision to consolidate was the inherent inefficiency in having numerous incompatible organizations performing virtually identical functions on dozens of different financial systems.

DFAS is supported by approximately 27,000 people and is located in five major centers and more than 300 field offices [Ref. 21]. In December 1992, DFAS took over responsibility for 332 installation finance and accounting offices and today consists of a headquarters and five centers (OPLOCs). Figure 4-3 below shows the current configuration.

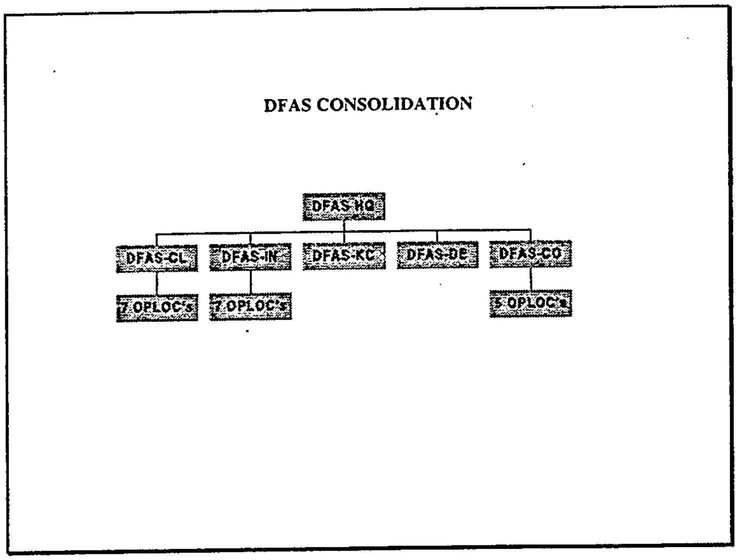

Figure 4.3. DFAS Consolidation [Ref. 2]

The workload of DFAS is enormous:

> On the business end for the FY ending 1998, DFAS processed a monthly average of 9.8 million payments to DoD personnel; 1.2 million commercial invoices; 600,000 travel voucher/settlements; 500,000 savings bond issuances; and 120,000 transportation bills of lading. The agency's monthly disbursements total approximately $24 billion. [Ref. 21:p. 1]
>
> On the average, vendor payment operations at DAOs process approximately 55 million transaction (nearly 12 million contracts and modifications, 19 million receiving reports, and 15 million invoices) to disburse more than 9 million payments totaling more than $30 billion a year. [Ref. 18:p. 3]

The current DFAS system is dynamic in its attempt to improve performance and meet customer needs. Below are the 1999 DFAS goals:

- Support the warfighter by reducing the cost of our operations
- Improve quality-timeliness-accuracy of outputs
- Meet or exceed all deliverables for the Agency Performance Contract
- Strengthen internal controls & elevate fraud awareness
- Implement the DFAS information infrastructure and corporate database
- Eliminate Twenty Legacy Systems [Ref. 21]

Section C of this chapter stated the common problems found throughout the DoD's vendor payment systems prior to consolidation. DFAS implemented several policies and changed procedures to correct some of the deficiencies. The DoD IG and the GAO have conducted several audits of the DFAS finance and accounting systems since 1991. The following is a list of the primary problems associated with the DFAS payment system uncovered in the various audits after the consolidation took place.

1. Slow Progress in Reduction of Problem Disbursements

> The Problem Disbursements Program Management Office established at DFAS in 1998 carried out limited efforts to identify causes and solutions for problem disbursements. DFAS Center personnel and financial managers of the DoD Components have spent much time and effort reviewing the causes of problem disbursements and developing courses of action to reduce their creation. However, they have not succeeded in eliminating existing problems disbursements and preventing the creation of new problem disbursements. DFAS did not take sufficient actions to fully determine the underlying causes of problem disbursements. Consequently, problem disbursements continue to be created. In January 1999, DFAS Headquarters began to require each of the DFAS Centers to identify the underlying causes of and completed actions for problem disbursements that had been researched and corrected. [Ref. 1:p. 9]
>
> The DFAS Cleveland Center reported significant reductions in problem disbursements for the Navy between June 30, 1996, and June 30, 1998. UMD's decreased from $6 billion in June 1996 to $4 billion in June 1998, a reduction of $2 billion dollars (33 percent). NULO's decreased from $2.5 billion in June 1996 to $1.7 billion in June 1998, a reduction of $.8 billion (32 percent). Although increased management emphasis resulted in the reduction in problem disbursements, about $1.2 billion of the $2.8 billion decrease in problem disbursements was related to the Navy discontinuing research on problem disbursements...Also, about $1.9 billion of the $5.7 billion was related to disbursements that were made before April 1, 1994. [Ref. 1:p. 11]

The likelihood of locating the required supporting documentation to research and resolve these problem disbursements diminishes with time. The risk of fraudulent vendor payments in problem disbursements remains high because DFAS is unable to determine the validity of the disbursement if it cannot be matched with valid accounting and supporting documentation.

2. Incorrect Recorded Obligations

> Auditors found that recorded obligations included amounts that were no longer correct or were unsupported. Specifically, at the Air Force, an estimated $4.3 billion of a $34 billion balance in obligations was found to be incorrect or unsupported. For example, obligated balances may not have been adjusted when goods or services were delivered at a lesser cost or when contracts were modified.
>
> In limited tests, the Naval Audit Service found that $101 million of $592 million of unliquidated Navy contract obligations, or approximately 17 percent, were incorrect. Army auditors also discovered evidence of unsupported obligations but were unable to quantify the extent of the problem. [Ref. 24:p. 21]

The risk of fraudulent vendor payments being made is extremely high, especially for the obligations that cannot be supported. Are the errors in recorded obligations intentional or non-intentional? A certain amount of error is inevitable. However, errors that go unchecked can possibly mean funds are being intentionally diverted.

3. Reconciliation Not Adequately Performed

DoD's records should be reconciled with Treasury records. As of September 30, 1998, a comparison of DOD's and Treasury records showed the absolute value of unresolved differences was $9.6 billion, of which $7.4 billion related to checks disbursed [Ref. 24:p. 21]. The GAO states that the difference between the two can result from (1) DoD delays in reporting transactions to Treasury, (2) Treasury delays in posting transactions to DoD accounts, and (3) errors or fraud.

Reconciliation's are a key control to combating possible fraud. Until these transactions are posted to the proper appropriation account, the department will have little assurance that the collections and adjustments recorded are authorized transactions, and that their disbursements do not exceed appropriated amounts.

4. Improper Contract and Vendor Payments

Auditors have long reported DoD's inability to make accurate contract and vendor payments.

> In the 5 fiscal years starting in 1994 through 1998, defense contractors returned about $4.6 billion to DFAS Columbus Center due to overpayments caused by contract administration actions and payment processing errors. [Ref. 21:p. 25]

> In compiling the Navy's FY 1998 financial statements, DFAS identified a negative (debit) accounts payable balance of $3.6 billion [Ref. 24, p. 25]. Typically, these negative accounts payable balances are due to overpayment or duplicate payment to vendors or contractors; however, DFAS did not conduct an investigation to determine the cause of the negative balances. Instead, DFAS and the Navy made unsupported adjustments of more than $6 billion to bring the accounts payable balance to the reported credit balance of $2.4 billion. [Ref. 24:p. 25]

An August 1998 Naval Audit Service Report identified $6.2 million in duplicate and erroneous Navy vendor payment out of $369.2 million tested [Ref. 24:p. 26]. Naval Audit Service concluded that these improper payments were caused by a lack of written policies and procedures for certifying and processing vendor invoices, certifying officer errors, accounting technician data input errors, and payment by two different paying activities for the same goods and services.

The current DFAS configuration has serious issues that need to be resolved. DFAS has developed and continues to implement policies and procedures to reduce the risks of fraudulent, erroneous, and duplicate payments and improve the overall quality of service.

F. COMPUTER TECHNOLOGY AND VENDOR PAYMENTS

Since FY 1990, DFAS has worked on numerous initiatives aimed at reducing or eliminating in-transit disbursements and problem disbursements. The emphasis has been on changing existing practices to accelerate the posting of disbursements and collections to accounting systems and to improve the accuracy of disbursing and accounting information. As part if the DoD's financial management reform, DFAS is adapting and adopting successful business practices from the private and government sectors. DoD intends to make its business practices simpler, more efficient, and less prone to error. A primary focus has been the move toward a paperless financial system. The focus originated from the concern for the massive paperwork flow required in the transaction cycle (See Chapter IV, Section B). The paperless system will reduce the cost of doing business for DoD. Many invoices were paid late, with accumulated interest, because too many invoices were on-hand and not tracked or prioritized by payment due date [Ref. 22:p. V-27]. Computer technology is one of the major forces which enables the DoD to achieve the desired cost and quality improvements in financial management. Computer technology in the form of Web Invoicing System (WinS), Electronic Data Access (EDA), Electronic Document Management (EDM), Electronic Data Interchange (EDI), and Electronic Funds Transfer (EFT) are the five avenues pursued by DFAS to promote the paperless exchange of financial information.

1. Web Invoicing System (WinS)

WinS enables the current paper based vendors to send invoices electronically with little or no cost. Vendors enter their invoices into templates on a DFAS owned Web server that processes and routes the invoices electronically but eliminates the normal telecommunications cost associated with EDI. The risks associated with WinS are the validity of the electronic invoice. Although this initiative decreases the time a vendor invoice reaches a paying station, the invoice still must be validated. Accounting technicians must ensure the receiving report is available and the invoice has a legitimate contract number in the pay system. Controls must also be in place to ensure that the invoices cannot be sent electronically to more than one paying station.

2. Electronic Data Access (EDA)

EDA uses Internet and World Wide Web technology to share documents across departments. EDA offers read-only access to official contracts and modifications, vouchers, Government Bills of Lading and accounting and finance documents in a common file format that eliminates the need for DoD users to maintain hard copy files. It reduces the need to print, mail, file, and manage paper and is designed to integrate with other electronic document initiatives. As long as the data cannot be manipulated by unauthorized personnel, this initiative appears to have a low risk. It is beneficial in that it decreases the risk of historical financial data being lost. Users can view the contract data and retrieve whatever information meets their need and not worry about handling hard copy file and risking misplacing the information.

3. EDM

EDM is designed to convert paper documents into electronic images and to automate the processing of these documents. It involves the collective application of three tools: imaging, electronic foldering, and workflow. Together these tools automate the presentation of financial and accounting material. Again, the risk here involves the validity of the data and the extent to which the data can be manipulated.

4. EDI

EDI is the computer to computer exchange of routine business information in a standard format. The EDI transaction sets eliminate the need to re-enter critical contract data in the contract pay system and financial data in DFAS administered accounting systems. This capability will help eliminate the feeder system problem, where data from one vendor pay system is translated incorrectly to another system and not checked for accuracy. There appears to be little or no risk of fraudulent payments with this capability due to the edit controls in the process. Implementing EDI invoicing capability, coupled with increased use of EFT, have been major factors in decreasing errors and improving payment processes [Ref. 26:p. 1]. However, access to the data and the ability to manipulate the data still must be strictly controlled.

5. EFT

EFT allows vendors to receive payment of funds electronically by registering their financial institution account information with DFAS. EFT is required for most contracts resulting from solicitation issued on or after July 26, 1996. EFT is reducing the costs of disbursements [Ref. 27:p. 5].

> Over 91 percent of DoD civilian employees and military members paid by DoD have their pay directly deposited into their accounts. The Direct Deposit participation rate for travel payments has increased from 17 to 48 percent. In 1996, 57 percent of the DFAS major contract payments were by EFT. This accounted for 81 percent ($54 billion) of total contract dollars disbursed [Ref. 26].

EFT is a positive capability if and only if the payments are accurate and have been prevalidated. Although these advances reduce costs and speed up the vendor payment process, the risk of fraudulent vendor payments will remain high if the payments are not validated and if data can easily be manipulated. These risk factors must be considered in the design and use of these technological advances.

G. DFAS INITIATIVES AND RISKS OF FRAUDULENT PAYMENTS

Due to weaknesses in finance and accounting, DFAS has begun the implementation of several initiatives designed to increase the accuracy of disbursing and accounting information.

1. Centralized Disbursing

The goal of centralized disbursing is to centralize all disbursing functions at one site, using one disbursing station. Centralized disbursing requires the data to be entered only once, thus reducing chances of input errors. In addition, a point of contact is identified when entering centrally disbursed transactions. The point of contact enhances quicker research resolution of problem disbursements. Currently, centralized disbursing does not prevalidate disbursements with obligations. However, another initiative, the Operational Data Store, will allow centralized disbursing to prevalidate payments. The DFAS Indianapolis Center began implementing centralized disbursing in April 1996 [Ref. 1:p. 28]. Eventually, it is to be fully implemented throughout DFAS.

The risk of fraud in centralized disbursing, assuming the data in the system is valid, is proportionate to the disbursing agent's ability to manipulate data (i.e. erase, add, delete, alter, and create). Routines in the computer will automatically detect differences in the voucher amount and disbursed amount, so this type of manipulation is not likely. Another risk is lack of segregation of duties. Management must ensure that the disbursing agent does not have access to the systems that input and transmit the automated invoice, receiving documents, and vouchers.

2. Defense Cash Accountability System (DCAS)

The DCAS consolidation initiative is the system selected by DFAS to be the single cash accountability system for the DoD. DCAS will replace the disparate accounting systems currently used throughout DoD. It is designed to improve the timeliness of recording in-transit disbursements by electronically transmitting collections, disburse-ments, and reimbursements between DFAS and accountable stations. In addition, transactions will be subject to edits that will improve the acceptability of the transactions into the accounting systems. Deployment of Phase 1 of the DCAS occurred in March 1999 [Ref. 1:p. 28].

The DCAS consolidation initiative is designed to correct weaknesses that have a critical impact on financial operations or data that impacts or involves violations of statutory requirements, fraud, or other criminal activities that go undetected [Ref. 22]. The risks of fraud surrounding the use of DCAS involve the extent of data manipulation and system access. Prevalidation of all data before it is entered into the system will be critical if this singular system is to be effective.

3. On-Line Payment and Collections

The on-line payment and collection system establishes a standardized interagency billing and adjustment procedure, using a telecommunications network. The system allows disbursement and collection transactions to be routed to accountable stations within 24 to 72 hours. This practice reduces in-transit disbursements. The first trading partnership agreements between DFAS organizations were signed in September 1997 [Ref. 1:p. 29].

The risk of fraud with On-line Payment and Collections involves the validity of the payable or receivable.

4. Prevalidation

The prevalidation process requires disbursing officials to determine, before making payments, that each line of accounting to be charged represents a valid obligation, and that the unliquidated obligation balance is equal to or greater that the proposed disbursement. This process is the most important initiative in fighting fraudulent vendor payments. How is prevalidation accomplished? In order for pre-validation to take place, accounting technicians must certify the validity of the actual invoice before making the payment. With electronic receipt of the invoice from vendors, accountants cannot blindly approve a disbursement. The transaction must be validated by the receiving command electronically or by mail. Currently, most military commands are not capable of transmitting receipt of goods information electronically [Ref. 26]. Although many vendors may be able to transmit invoices electronically, a large amount of paper flow remains a part of the system. This paperflow causes payment delays, loss of paperwork, etc. Controls must be in place to also ensure that the vendor does not forward invoices to more than one accounting station, causing duplicate payments. The importance of a unique job order number and the ability of financial systems to cross verify accounts resolve this problem. So the process of prevalidation must be carefully thought out and supported by computer systems that can incorporate adequate controls. This is how prevalidation should be done. Automatic prevalidation should follow the same steps. With the billions of dollars paid to vendors and contractors by DoD on a yearly basis, the need for automation is critical. Nonetheless, with the emphasis on getting the payments to the vendors as quickly as possible and making payments without verifying receipt of goods from the customers, paying stations often do not take these steps. These are primary reasons for the problem disbursements and fraudulent payments that get through the vendor payment systems.

DFAS Centers, in order to comply with the Prompt Payment Act, use Fast Pay which, is an exception to normal payment rules. The Prompt Payment Act requires all federal agencies to pay bills in a timely manner, pay interest when late, and take discounts only within discount periods. It is primarily used by fleet units. Vendor invoices are mailed directly to a paying office and payment is received within 15 days. The Fast Pay system overrides the control of verification of receipt of goods from the receiving agency in order to meet the needs of the fleet. This goes against the DoD effort to prevalidate all vendor/contract payments before payments are disbursed.

The Under Secretary of Defense, Comptroller USD (C) developed two plans for matching disbursements to particular obligations before making disbursements. The first plan provides a reasonable approach for lowering the threshold for prevalidation to $1 million from $5 million dollars at the DFAS

Columbus Center. The second plan provides for lowering the threshold to zero dollars by October 1, 1998, for all contract and vendor payments paid by other than the MOCAS system. The second plan has not happened. Now, for contracts awarded before FY 1997, contract payments made by the MOCAS system would be incrementally decreased to zero by June 30, 2000. For contracts issued after October 1, 1996, the DFAS Columbus Center was prevalidating all invoices valued at $2,500 or more using the MOCAS system. However, on December 17, 1998, the USD (C) temporarily raised the threshold to $500,000. On March 1999, the temporary increase in the threshold was extended for another 90 days.

DoD intends to prevalidate all payments to contractors and vendors after system enhancements are made. In the meantime, the risk remains extremely high that fraudulent vendor payments are being made because of the lack an effective prevalidation system and the billions of dollars in problem disbursements.

5. Transaction For Other Cell

The Transaction for Other Cell within a paying center receives the invoices from contractors and vendors and accesses the entitlement system supporting the lines of accounting associated with the invoices. This significantly reduces the time transactions are in transit between the disbursing station and the accountable station and reduces, but does not eliminate problem disbursements. Initial use of Transaction For Others Cell began in April 1997, and in April 1998, DFAS expanded its use. About 25 of the 233 sites connected as of June 30, 1998, had been connected before April 1, 1998 [Ref. 1:p. 29]. This initiative is an important step in the prevalidation process. Accounting technicians must ensure they do not approve a payment on an unmatched job order number.

THIS PAGE INTENTIONALLY LEFT BLANK

V. OPERATION MONGOOSE

A. INTRODUCTION

Operation Mongoose is the Department of Defense Fraud Detection and Prevention Unit. It was founded in 1994 by the Under Secretary of Defense, Comptroller, Dr. John Hamre, who is now the Deputy Secretary of Defense. It was established to minimize fraud against the financial assets of the DoD.

Operation Mongoose is the first mulit-agency program formed with a national scope to examine possible financial fraud. It is comprised of a partnership between DFAS, Defense Manpower Data Center (DMDC) and the DoDIG. Other agencies are also involved, including the U.S. Secret Service, Department of Veterans Affairs and the Social Security Administration.

Operation Mongoose examines retired and annuity pay, military pay, civilian pay, transportation payments, and vendor payments. Since its inception, it has analyzed tens of millions of financial transactions to detect potential cases of erroneous and fraudulent payments.

> Tangible results as of June 1998, include the identification of $12.7 million dollars in erroneous payments, hundreds of cases for Defense Criminal Investigative Services (DCIS) investigation and resulted in several cases for criminal investigation. [Ref. 3]

B. FRAUD DETECTION METHODS

Using the data storage and processing capabilities of DMDC, Operation Mongoose has access to payment and supporting data on several different computer systems from more than 300 sites nationwide. By having a central point of data collection and processing, research time is drastically reduced. Information obtained from the various DoD payment systems is matched against indicators developed by subject matter experts from DFAS, DMDC and the DoDIG. These "smart" matches performed by DMDC help identify anomalies in the data which may indicate fraud or internal control weaknesses.

1. Vendor Pay Files

The vendor pay files contain installation commercial accounts payable information from the Services. The accounts payable data is the bridge between the contracting systems and the disbursing systems. These systems reconcile the requisitions with the actual receipt of goods to accurately compute the vendor payment. DMDC receives the data from four different database systems from over 100 submission sites.

The automated financial systems that produce these submissions are the Automated Financial Entitlement System (AFES), the Computerized Accounts Payable System (CAPS), the Integrated Accounts Payable System (IAPS), and the STARS-FL. The data consists of extracts from the various database tables from each of the vendor pay systems. The files provide invoice, receipt and voucher information to the contract line level such as: unit price, quantity ordered, merchandise receipt and costs, dates of receipt, freight charges, vendor name, address and payment preference, item description, voucher number, and some accounting data.

2. Vendor Database

The vendor database contains government vendor information for all federal agencies. The data is collected at various agencies and validated before submission. Data is submitted from several sources including the Central Contract Registry (CCR), Federal Procurement Data System (FPDS), Defense Logistics Agency (DLA), Commercial and Government Entity (CAGE) file, and the Small Business Administration's Procurement Automated Source System (PASS). The validation sources include Dun & Bradstreet DUNS number, Defense logistics Agency CAGE codes, and Taxpayer Identification Number (TIN). The files also contain information which would indicate the vendor's status such as "Active" or "Debarred". The data is collected and archived in the data warehouse to facilitate pattern matching and identification.

3. Disbursing Files

The Standard Installation-Level Automated Accounting and Financial Reporting System (STANFINS) Redesign Subsystem 1 (SRD-1) consists of disbursing files from over 30 installation and center-level disbursing offices. DFAS centers submit a suite of thirteen files from the commercial accounts payable portion of the database. These files contain records for each accounts payable voucher and check/EFT payment processed in SRD-1. The files include information such as interest charged to an appropriation, the amount and accounting classification data for each line item on each voucher, discount and invoice data for a particular payment, and check and EFT payment data for a particular payment made to a particular vendor.

4. Contracting Files

The contracting files include separate submissions from installation contracting officers of the Services and Defense other defense agencies. There are over 200 of these submission sites. The automated financial database systems that produce these submissions are the Automated Procurement and Accounting Data Entry (APADE), the Base Contracting Automated System (BCAS), the Standard Army Automated Contracting System (SAACONS), and the Base Operating Support System (BOSS). The files provide general and detailed procurement information, such as contract number, award date, award amount, discount data, modifications and line item data to include requisition number, quantity, unit price, description, and accounting data. The files also include vendor information, such as name, address, ship-to-address, remit-to-address, tax and ID codes.

Operation Mongoose uses these files, the vendor disbursing files, the vendor database, and the vendor pay files to detect fraud by computerized routines that compare data from each of the database systems. To date, Operation Mongoose has not detected any incidents of fraud using this technique. They have, however, identified several cases of duplicate payments and erroneous payments. Also, they have provided supplemental data to assist investigating agencies on fraud cases that have been uncovered by sources outside of Operation Mongoose [Ref. 32].

C. DATA MINING

Data mining is a new, complex computer tool that uses knowledge discovery to look at very large data sets to search for and identify hidden data, patterns, and trends. An analysis of data anomalies is performed in search of indicators sufficient to warrant investigation and to identify possible individual intrusion into the financial systems for illegal personal gain.

Operation Mongoose contracted for data mining software in June 1999. The software is designed for a variety of applications including fraud detection. Once the software is in place, vendor payments will be the first to be analyzed [Ref. 31]. Data mining is a promising tool for Operation Mongoose to improve it's fraud detection effectiveness.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. FRAUDULENT VENDOR PAYMENT CASES ANALYSIS

A. INTRODUCTION

This chapter examines data from known DoD fraudulent vendor payment cases. The analysis involves cases uncovered in DoD since 1990. A total of sixteen cases are discussed. All cases are analyzed in light of their management control weakness. The first three cases are described in detail due to the high visibility they received when uncovered. Thirteen cases contain a brief summary of the events that took place. Six specific data elements from each of the cases are extracted and displayed for further analysis. The display also includes data elements from five additional Army cases.[1]

B. CASE DATA

The DoD fraud cases are as follows:

1. Case #1

> In the fall of 1992, [a civilian employee] Contractor's Technical Representative (COTAR) successfully encouraged [certain] contract personnel to bill the government over $300,000 for services that were not rendered. The contractor provided office automation hardware, software, maintenance, training, and contractor support services for the Air Force. He [the employee] attempted to obtain these funds by directing the contractor to pay a non-existent subcontractor for consulting services based on a bogus subcontractor invoice that he supplied. When the contractor's administrative

[1] The summary information for some Army cases was not available.

> personnel learned of the billing incident, the contractor conducted an internal investigation and returned the checks to the government.
>
> After [the contractor] employees refused to participate in the scheme involving the bogus subcontractor invoice, [the civilian employee] executed another plan in December 1992, without the contractor involvement, by which he created and submitted 11 bogus invoices totaling $504,941. In January 1993, the Air Force issued payment checks for the invoices and mailed them, unwittingly, to a post office box that the perpetrator had opened. In February 1993, he deposited the $504, 941 into two bank accounts he had opened using the contractor's name. The perpetrator's theft was detected after officials of the bank in which he had deposited the checks became suspicious of what they considered to be unusually large transactions and reported them to the U. S. Secret Service. [Ref. 33]

The contractor, after investigating the perpetrator's initial attempt at defrauding the government, considered the actual fake invoices to be billing errors and returned the checks to the Air Force. The incident was not questioned by anyone in the Air Force or at DFAS. The perpetrator's second attempt was successful. The 11 fake invoices he submitted subsequent to his previous attempt were in the name of the contractor, using its vendor account number. The fake invoices were accepted in the vendor payment system. Why? The perpetrator forwarded a false certified receipt of services with the fake invoice. The contract number was valid and in the system, so, on the surface, the transaction appeared normal. The specific controls violations include segregation of duties, recording and documentation, and supervision. The perpetrator had broad authority to request contract amendments, order goods and services, receive and accept goods and services, and approve payment for the items received–thereby violating segregation of duties. Adequate supervision was also violated. The supervisor told investigators that she allowed the COTAR to perform these duties independently without close supervision [Ref. 35]. Recording and documentation controls were violated when the checks were forwarded to the post office box that did not match what was in the computer database. Standardization of data entry is one of the key factors in adhering to the proper recording and documentation specific controls. If the discrepancy had been noticed, the contractor would have received a form to verify the remittance address, and they would have been given the correct procedures/paperwork required to change that address. The fraud should have been detected through this communication/and verification between DFAS and the contractor.

> According to the accounting and finance certifying officer, it was the policy at the time to make payments to the company and address indicated on an invoice (regardless of what the computer system indicated as the contractor's address). [Ref. 33:p. 11]

2. Case #2

> In 1990, at Robins AFB investigators uncovered a complicated fraud scheme involving $2 million, nine Air Force employees, four vendors, and six vendor employees.... The first perpetrator was exposed by two suspicious hardware store vendors. The perpetrator, an Air Force employee, ordered materials from the two vendors, received the materials, returned them, and requested a line of credit

> instead where he purchased personal items. The two vendors became suspicious and called the Air Force Office of Special Investigations. The first perpetrator admitted to the scheme along with his supervisor, who was aware of the fraud.
>
> Further investigation revealed that the supervisor succeeded in defrauding the government of more than $200,000 by conducting the same scheme at a third vendor run by a retired Air Force Master Sergeant. After extensive questioning, the third vendor revealed that from 1985 to 1990, he colluded with seven other Air Force employees to defrauded the government of $1. 8 million.... He also set up a money laundering operation for the stolen money through a friend's company. One employee who worked in the contracting office handled small purchase requests from civil engineering. He colluded with the third vendor by disclosing the bids of competitors so that the vendor could bid just under the competitors and receive the contract. This [contracting official] accepted $95,000 in bribes from the vendor. Another [employee supervisor] accepted $27,000 in cash and property from the vendor in exchange for remaining silent about his subordinate's circumvention of the required contract procedures.
>
> The schemes worked in this manner. The perpetrators prepared a purchase request for a fictitious requirement and submitted it to the contracting office. The purchase request identified the vendor participating in the scheme as the recommended source. A contract was issued to the vendor. The perpetrators then went to the vendor and signed a form certifying that the items ordered on the contract had been delivered when in fact they had not. The vendor sent an invoice with the false delivery certificate to the Robins AFB finance office which then paid the vendor. The vendor arranged to keep a thirty percent markup for profit and overhead. He shared the balance with the Air Force employees. [Ref. 34]

The difficulty in detecting any fraud in this case is the high level of collusion. There were several people in positions of authority receiving bribes and participating in the scheme over the course of five years. This scheme may not have been uncovered if it were not for the two vendors who happened to know each other and were discussing the suspicious behavior of an Air Force employee over lunch. The specific standard violations include segregation of duties and supervision. The responsibility of receiving goods should have been separated from the requester. If that had been done, the receiver would be able to verify that although a contract was let, no actual goods or services were received. I hesitate to say that supervision was inadequate because of the level of collusion. A very conscientious supervisor still may not have detected this level of corruption. The Air Force employees who committed the fraud followed the correct procedures by submitting a purchase request for items to the contracting office with a recommended source so no discrepancy in any paperwork would have been noted. A higher level supervisor would have to physically see that the goods were not received. That is not likely because management normally delegates this responsibility to lower level supervisors and employees.

3. Case #3

> An Air Force Sergeant was convicted of fraudulent activities at two locations. The first known location where fraudulent payments were made was Castle AFB, California, between October 1994 and May 1995. The Staff Sergeant, who was the Chief of Material in the Accounting Branch, had broad access to the automated vendor payment system, which allowed him to enter contract information, including contract numbers, delivery orders, modifications, and

obligations as well as invoice and receiving report information and remittance addresses.

The Staff Sergeant used this broad access to process invoices and receiving report documentation that resulted in eight fraudulent payments totaling $50,770 that were identified. The invoices prepared by the Staff Sergeant designated the name of a relative as the payee and his own mailing address as the remittance address. Castle AFB closed in September 1995, and the Staff Sergeant was transferred to DFAS Dayton.

At DFAS Dayton, the Staff Sergeant was assigned as the Vendor Pay Data Entry Branch Chief in the Vendor Pay Division. As Vendor Pay Chief, the Staff Sergeant was allowed a level of access similar to the one at Castle AFB. Between November 1995 and January 1997, he prepared false invoices and receiving reports that resulted in nine fraudulent payments totaling $385,916. By designating the remittance address on the false invoices, the Staff Sergeant directed fraudulent payments to an accomplice.

He was also convicted of altering invoices and falsifying information in the vendor payment system- in violation of 18 U.S. C. 1001-to avoid interest on late payments and improve reported performance for on-time payments.

In February 1997, the Staff Sergeant was reassigned to DFAS Dayton's Accounting Branch and his access to the vendor payment system was removed. However, while assigned to the Accounting Branch, he created two false invoices totaling $501,851 and submitted them for payment in June 1997, using the computer password of another DFAS employee. His fraudulent activities were detected when, for an invoice totaling $210,000, an employee performing the Merged Accountability and Fund Reporting reconciliation identified a discrepancy between the contract number associated with the invoice in the vendor payment system and the contract number associated with the invoice in the accounting system. These two numbers should always agree. For this invoice, the Staff Sergeant failed to ensure that the contract cited was the same in both systems. [Ref. 35]

These particular acts of fraud occurred because of violations of segregation of duties, access and accountability for resources, recording and documentation. The fraudulent activity at Castle AFB was not detected until research was done upon the discovery of the two fraudulent payments at DFAS Dayton. At each command, the perpetrator had broad authority to manipulate contract data which he used as an opportunity to commit fraud. The level of access directly relates to the segregation of duties. The Staff Sergeant held the highest level access which allowed users to input or change contract data, information on obligations, invoices, and receiving reports, and remittance addresses. Proper and effective internal controls would preclude any individual user from having the ability to manipulate data to this extent. Without segregation of these duties and controls over access to the system, compensating controls should be in place, such as reviews of remittance address change activity and periodic verification of payment addresses with the vendors. Recording and documentation controls were violated because the data was not prepared faithfully, and remittance address and the address on file were different. This reinforces the need for data standardization. Nothing in the system alerted anyone of the discrepancy. In fact, if he had not made the mistakes in the accounting data, those payments probably would have made it through the vendor payment system. This reinforces the criticality of segregation of duties.

The falsification of payment documents to improve performance for on-time payments undermined the DFAS Dayton's internal control over payments and impaired its ability to detect or prevent fraud [Ref. 35]. According to authorities, the Staff Sergeant had also instructed his branch employees to falsify invoice dates in an effort to improve reported payment performance.

> This was done by (1) altering dates on invoices received from contractors, (2) replacing contractor invoices with invoices created using an invoice template that resided on DFAS Dayton personal computers used by vendor payment employees, and (3) throwing away numerous invoices. [Ref. 35]

4. Case #4

A military clerk in an accounting and finance office at Hanscom Air Force Base, Massachusetts, embezzled more than $316,000 by altering previously paid contractors claims and resubmitting them for payment. The clerk obtained a fictitious business license and opened a business bank account under the fictitious business name on the claim forms. He had the claims checks sent to a post office box from which he retrieved them and deposited them into the fictitious business bank account. The clerk's wife discovered the scheme and threatened to report the theft. The clerk later confessed the embezzlement scheme to a coworker[Ref. 33]

5. Case #5

A retired Navy chief petty officer and former Civil Service merchant mariner served as a supply officer aboard Military Sealift Command Ships. Between January 1989 and December 1992, he defrauded the Navy of over $3 million. He filed bogus invoices for materials allegedly supplied to the Military Sealift Command by a company that did not exist. DFAS mailed payments to a Norfolk, Virginia, post office box. His fraud was uncovered when someone noted that shipments and services were going to decommissioned ships. [Ref. 33]

6. Case #6

On three occasions at the Air National Guard Station, Birmingham, Alabama, a military comptroller fabricated payment vouchers using fictitious contract numbers and fictitious contractor names, resulting in $118,000 being sent to a bank account that the comptroller controlled. An accounting technician uncovered the scheme when he noted a discrepancy in the records…[Ref. 33]

7. Case #7

A military supply clerk at the Norfolk, Virginia, Naval Station submitted false claims to the Navy for supplies or services under the names of four legitimate companies and one that he had registered for the purpose of his fraud. All invoices were bogus, as no materials or services were ordered or delivered. He was discovered when the Norfolk Police Department, which was investigating him concerning the sale and/or possession of narcotics, seized his computer and found bogus invoices. The Norfolk police reported the matter to the Naval Criminal Investigative Service as a possible fraud…. He was ordered to make restitution of $83,576.63...[Ref. 33]

8. Case #8

Between December 1991 and August 1993, sixty-two unauthorized payments, totaling approximately $271,000, were fraudulently issued and cashed by two employees of the DFAS Indianapolis, Indiana, Center. Checks were issued in the names of various U. S. military retirees but were sent to addresses controlled by the two perpetrators. The checks were forged and negotiated using false identification at various check-cashing establishments. Subsequently, the two employees recruited others to participate in the fraud scheme. The checks made payable to the recruited individuals were negotiated at banks, and the recruits received a percentage of the proceeds. A complaint from a retiree who questioned the income amounts that the military had reported to the Internal Revenue Service triggered a review of the payment operations. The investigation resulted in the conviction of 12 individuals for theft of government funds…[Ref. 33]

9. Case #9

Between 1994 and 1997, a military member and a private citizen allegedly embezzled approximately $938,000 from the DFAS Dayton, Ohio, Center. The military member was a supervisor of the data entry personnel in the vendor pay section and allegedly created fraudulent invoices and checks payable to the private citizen. They then allegedly divided the proceeds. A technician who had no part in the scheme noticed a check made out to the private citizen for $210,000 when she was trying to discover the source of an automated input error. The check was suspicious, as it was for a large amount made payable to an individual rather than a business and the transaction did not match a valid contract...[Ref. 33]

10. Case #10

In late 1995, a civilian employee of the DFAS Cleveland, Ohio, Center diverted $11,000 by using electronic funds transfers to a bank account controlled by the employee and an accomplice. The employee diverted military retirement benefits by issuing two separate "one-time-credit" allotments, thus triggering the electronic transfer. The employee withdrew the diverted funds. The fraud was discovered as a result of a DFAS internal control that automatically generated reports on payments over a predetermined amount. When the report was reviewed, DFAS personnel questioned the payments...[Ref. 33]

11. Case #11

Between October 1994 and January 1996, a civilian DFAS accounting technician embezzled $28,940 in funds from DFAS-Tinker AFB, Oklahoma. The technician falsified educational expense vouchers using his wife's name as the payee and his own mailing address. The technician attached used copies of supporting documents from legitimate vouchers to support the fraudulent vouchers, knowing the certifying official would not verify the expenses or the identity of the claimant. The technician cashed the checks and used the proceeds to pay debts. The scheme was discovered after a confidential source provided information to law enforcement...[Ref. 33]

12. Case #12

In 1991, two military members assigned to the DFAS Indianapolis, Center conspired with seven individuals to receive approximately $37,000 in fraudulent benefits paid to beneficiaries of military personnel killed during Operation Desert Storm. One military member created the necessary paperwork within DFAS to issue checks against the accounts of deceased service members. The other military members recruited seven individuals to receive the fraudulent checks. These seven individuals each received a minimal portion of the proceeds for facilitating the embezzlement. The scheme was discovered as a result of an anonymous call to law enforcement. [Ref. 33]

13. Case #13

Between October 1994 and April 1997, a military pay supervisor and a private citizen at Fort Myer, Virginia, schemed to embezzle approximately $169,000 of government funds. The supervisor established a payroll account in the name of a fictitious military member. The supervisor used the ghost payroll account as a basis for issuing 57 electronic fund transfers to bank accounts controlled by the perpetrators. Sources outside DFAS reported the scheme. [Ref. 33]

14. Case #14

In 1993, a bookkeeper at Reese Air Force Base, Texas, embezzled more than $ 2 million dollars over three years without arousing suspicion of base officials or higher-ups in the chain of command at DFAS or the Air Force...[Ref. 37]

15. Case #15

In 1996, a payroll clerk at Robins Air Force Base, pled guilty to one count of embezzlement of public funds. [She] inputted false data into the computerized time and attendance system for overtime hours she did not work. From January 1994, through February 1996, she falsely input 1,849 overtime hours into the system so that she fraudulently received $25,764 in overtime pay...[Ref. 39]

16. Case #16

Employees of a management services contractor submitted false invoices to support payments for spare parts and for non-existent meals. The employees were directed to alter, falsify, and fabricate records used for accounting and inventory to cover up losses, thefts, and improper management. [The contractor] was fined $6.3 million dollars and debarred from doing business with the federal government for three years. [Ref. 40]

C. DATA COMPILATION

The following section compiles and summarizes six data elements from the 21 cases. The data are compiled to offer a better insight into actual fraudulent payments in DoD.

1. How Was the Fraud Committed?

The cases were analyzed to determine how each fraudulent act was committed. The categories include fraud committed using fake documents (false invoices, false certification of receipts, false purchase requests, and false vouchers), fake employees, and altered documents (overpayment, resubmission). Some cases involve more than one fraud type. See Table below.

Fraud Type	No. Occurred	Percentage
Fake Documents	21	76%
Fake Employee	4	14%
Altered Documents	3	10%

Table 6.1. How Fraud Was Committed [Refs. 32-39]

2. How Much Money Was Stolen?

The amounts stolen also include attempted amounts in cases where the fraud was discovered before checks were cashed. Below is the breakdown of the cases.

Amount Stolen	No. Cases	Percent
<100	9	43%
100-500	5	24%
600-1000	2	9%
>1000	5	24%

Table 6.2. Amounts Stolen ($ thousands) [Refs. 32-39]

3. How Was the Fraud Uncovered?

How the fraud was uncovered is broken down into two categories, external sources and internal sources. The internal sources include co-workers, internal audits (computer), confessions, and internal controls (accounting/disbursing procedures). The external sources include external controls (accounting/ disbursing procedures) outside of the organization, banks, and tips (unknown and known). In some cases the discovery source information was not available (unknown). See the following table.

Discovery Source	No. Cases	Percent
Internal:		
Co-workers	1	4%
Confession	2	9%
Internal Control	2	9%
External:		
External Control	3	13%
Banks	2	9%
Tips (Unknown)	3	13%
Tips (known)	7	30%
Unknown Source	3	13%

Table 6.3. Fraud Discovery Source [Refs. 32-39]

4. What Specific Standards Were Violated?

The primary violations involved access and accountability, supervision, segregation of duties, and recording and documentation. Most cases involved a combination of factors. Lack of segregation of duties was noted most often. See figure below.

Control Violations	No. Cases	Percent
Access/ Accountability	11	33%
Supervision	7	21%
Segregation of Duties	12	36%
Doc/Rec	3	8%

Table 6.4. Management Control Violations [Refs. 32-39]

5. What Was the Position of the Perpetrator (s)?

This category only includes whether the perpetrator was military or civilian. Most perpetrators were in positions of authority. See table below.

Status of Perpetrator	No. Perpetrators	Percent
Military	10	25%
Civilian	30	75%

Table 6.5. Status of Perpetrator [Refs. 32-39]

6. What Service Was Involved?

The fraud cases are broken down into their associated Services. Fraud cases that occurred at DFAS centers, accounting and disbursing stations were categorized based on the primary DoD agency they serve. See table below.

Service	No. Cases	Percent
Navy	3	14%
Army	9	43%
Air Force	8	38%
Air Nat Gd	1	5%

Table 6.6. Associated Service [Refs. 32-39]

These cases demonstrated how weaknesses in the management controls provide opportunities for employees to commit fraud fairly easily.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSIONS AND RECOMMENDATIONS

A. SUMMARY

This thesis shows that the effective use of management controls in the DoD vendor payment systems is imperative in the prevention and detection of fraudulent payments. It also demonstrates that the DoD vendor payment systems are vulnerable to fraudulent payments being made.

Chapter II provided an overview of fraud in general, including the factors that interact to determine whether a person will commit fraud. It provides a perspective on how DoD historically handled fraud issues and discusses the current issues surrounding fraud, waste and abuse. With several laws in place which provide a framework and guidance, DoD can endeavor to eliminate fraud and effectively manage its assets. The issue of validating problem disbursements must remain a priority because, otherwise, officials will not know whether these vendor and contract payments are legitimate and do not exceed legal limits.

Chapter III discussed the important issue of management controls. The keys to eliminating fraud are adherence to the general and specific controls as set forth in OMB Circular A –123. All DoD financial managers should regularly assess all their operations and procedures to determine risks and the consequent risk of failures of internal controls.

Chapter IV discussed the vendor payment systems in the DoD and how they function, the risk associated with the DoD pre-consolidated finance and accounting organization and current DFAS organization, the impact of computer technology on vendor payments, and current DFAS initiatives. Before consolidation, finance and accounting services in DoD had serious problems with the implementation of controls to reduce the risks of fraud. Auditors found major discrepancies throughout the systems. In many cases controls were not in place at all to reduce the risks of fraud. In other cases procedures were in place but not followed. The advances in computer technology provide advantages and a primary disadvantage to DoD finance and accounting. The advantages include the increased ability to process the billions of dollars in transactions more quickly, reduce paperwork, improve processes, store massive data, improve accuracy of accounting and financing, etc. The primary disadvantage of computer technology is the increased risk of creating fraudulent vendor payments if access and manipulation of data is not properly controlled. Auditors have found that too many employees continue to have unnecessary access to vendor payment systems [Ref. 25]. The DFAS has begun the implementation of several initiatives, which are designed to increase the accuracy of disbursing and accounting information. These initiatives appear promising because they will facilitate DoD's move toward using a single system for accounting and finance versus the variety of systems currently in operation.

Chapter V discussed the DoD fraud detection and prevention unit, Operation Mongoose. Operation Mongoose has identified numerous erroneous payments. It has also provided supplemental and additional information to investigators in several fraud cases. A promising new technique called data mining will allow Operation Mongoose to look at very large data sets to search for and identify hidden data, patterns, and trends. Data mining promises should be instrumental in the ability of Operation Mongoose to detect fraud.

Chapter VI discussed 21 actual fraud cases uncovered throughout the DoD. The analysis and summary of data from these cases clearly demonstrate the importance of effective use of management controls. These cases show that the primary means of committing fraud were fake documents. This finding is logical because of the nature of this type of fraud. The majority of the money stolen in these cases was under $100,000. The Association of Certified Fraud Examiners (ACFE) reports a median loss of $250,000 by managers who commit fraud [Ref. 4]. The majority of the cases was uncovered by an external source and not by internal control mechanisms. This further demonstrates the lack of effective controls pervasive throughout DoD. In each case segregation of duties was the primary weakness. The other internal controls were not far behind. These finding are consistent with GAO and DoD findings [Refs. 4, 35]. The majority of the cases involved civilian employees. The cases do not necessarily reflect the population of fraud cases because of the small sample size. These are not all of the fraud cases ever uncovered by DoD. This sample of cases is presented only to provide a better insight into fraud in DoD. Although the Air Force owned most cases, that does not mean that its employees commit the most fraud. Information on the Air Force cases was more readily available.

B. RECOMMENDATIONS

The issue of fraudulent payments in DoD is complex due to the mere size of DoD and the billions of payments made each year to vendors and contractors. Nonetheless, I recommend the following:

- Strengthen payment processing controls by establishing separate organizational responsibility for entering (a) obligations and vendor information, (b) invoice and receiving report information, and (c) changes in remittance addresses.

- Identify the minimum number of employees needing on-line access to vendor payment system, determine whether the access levels given to each user are appropriate for the user's assigned duties, and remove access from employees who are no longer assigned to the specific function.

- Managers assess the internal controls over vendor payment process and establish and monitor control regularly.

- Implement initiatives that consolidate DoD financing and accounting to a single system.

C. ANSWERS TO RESEARCH QUESTIONS

1. How has the consolidation/organization of the vendor payment system impacted the detection and prevention of fraudulent vendor payments?

The consolidation of finance and accounting offices has had both a positive and negative effect on the prevention and detection of fraudulent vendor payments. On the positive side, consolidation has reduced the widespread, satellite locations of accounting and finance offices. The formation of the OPLOC's and their responsible areas increased accountability and oversight, which is a management control tool. The disadvantage is that, in the transition, a massive amount of historical data and vendor information was lost or destroyed. That made it difficult to validate payments and maintain historical files. A portion of the current problem disbursements is due to this lack of documentation. This is a problem especially in the Navy, where approximately $1.9 billión in problem disbursements were made before April 1, 1994 [Ref. 1]. Another disadvantage is the loss of personnel during the phases of consolidation. DFAS, despite reductions in DoD personnel and resources, has an enormous workload. This reduction in personnel may be partially responsible for the weaknesses in the segregation of duties control. With less personnel and a large work load, employees sometimes take on more responsibility and are required to perform all aspects of a job in order to complete the work.

2. How has computer technology impacted the detection and prevention of fraudulent vendor payments?

Computer technology has been instrumental in DoD's attempt to become efficient and migrate toward a single accounting and finance system. Management control processes can be programmed into computers to assist in the prevention and detection of fraud. Some of the DFAS initiatives are design for this purpose. In one of the fraud cases discussed in Chapter VI, a computer program alerted an accounting technician to a discrepancy in computerized data. That prompted an investigation and subsequently uncovered a fraud scheme. Detecting and preventing fraud using computer technology will become increasingly important in the future. DoD plans to prevalidate all vendor invoices before payments are made. It will depend on computer technology to accomplish this goal. Currently, the access to and ability to manipulate data is widespread among many DoD employees. Once this access and ability to manipulate data is adequately controlled, computer technology will increase its usefulness in the detection and prevention of fraudulent payments.

3. How effective are financial management instructions/controls in detecting fraudulent vendor payment?

The general and specific controls established in OMB Circular A-123 are proven methods of deterring fraud. These standards are recognized and used throughout the business industry. While no controls are guaranteed to deter fraud all the time, effective controls significantly reduce the risks of fraud. Weak or nonexistent internal controls, as demonstrated in the case analyses, prove to be quite dangerous. However, effective controls mean the active use of those controls. Having controls in place and not following them is equivalent to not having any controls. Managers must ensure that controls are implemented, periodically monitored, and adjusted as necessary.

4. What, if any, are the geographical, technological, or demographical trends in fraud cases already uncovered in DoD?

a. Geographical

In the 21 cases discussed, there appears to be no pattern in the actual location of the fraud. The fraud occurred at different regions and at different command levels.

b. Technological

Most of the cases discussed involved the use of computer systems that facilitated the fraud. The use of computers takes away the ability to check signatures and examine documents to determine any alterations. However, there are controls that can and should be programmed to achieve the same level of control.

c. Demographical

There was not enough information to determine any trends in the sex, age, race, or exact rank of the offender.

D. RECOMMENDATIONS FOR FURTHER STUDY

1. Problem Disbursements

Analyze and develop ways to resolve problem disbursements and prevent new ones from occurring.

2. Management Controls

Review management controls procedures in the DFAS organization and make recommendations for improvements.

LIST OF REFERENCES

1. Department of Defense, Office of the Inspector General, Trends and Progress in Reducing Problem Disbursements and In-Transit Distribution, GPO, Washington, DC, 16 April 1999.

2. Hleba, T., Practical Comptrollership, Naval Postgraduate School, Monterey, CA, 28 August 1998.

3. Defense Finance and Accounting Services, "Operation Mongoose," [http://www.dfas.mil], November 1998.

4. Association of Certified Fraud Examiners, "Report to the Nation on Occupational Fraud and Abuse," [http://www.cfenet.com], June 1999.

5. Bennet-Thrasher& Company, "Prevention-The Best Weapon Against Fraud," [http://www.bennett-thrasher.com], March 1999.

6. The Chubb Cooperation, "White Collar Crime Loss Prevention," [http://www.chubb.com].

7. Revilin, A. M., Circular No. A-123, [http://www.whitehouse.gov/OMB/circulars/a123/a123.html], 21 June 1995.

8. Office of Management and Budget, "Standards of Conduct for Employees of the Executive Branch," [http:/www.nsf.gov/home/pubinfo/coi/5cfr2635], 6 August 1992.

9. Groves, I. F., Fraud Awareness and Internal Controls, paper presented to the Association of Military Comptrollers Professional Development Institute, 21 June 1999.

10. Apostolou, N.G., Handbook of Government Accounting and Finance, John Wiley & Sons, Inc., 1988.

11. McKinney, J. B., and M. Johnston, Fraud, Waste, Abuse in Government, ISHI Publication, 1986.

12. Department of Defense, Office of the Inspector General, DoD Fraud Hotline Generally Affective But Some Changes Needed, GPO, Washington, DC, 21 March 1999.

13. Krushinski, L. J., "From the Director DFAS-CL," Navy Comptroller, 2nd QTR FY 99, Volume 10, Issue 2, January 1999.

14. Department of Defense, Office of the Inspector General, Inspector General, DoD, Oversight of the Naval Audit Service Audit of the Navy General Fund Financial Statements for FY's 1997 and 1996, GPO, Washington, DC, 7 April 1999.

15. Abel, David, "GAO Slams Pentagon Fraud, Waste, Abuse," Defense Weekly, 1 February 1999.

16. Department of Defense Inspector General Memorandum for Under Secretary of Defense (Comptroller) and Chief Financial Officer Director, Defense Finance and Accounting Service, Subject: Endorsement of the Disclaimer of Opinion on the FY 1998 Department of the Navy General Fund Financial Statements (Project No. 8FC-2030), 1 March 1999.

17. United States General Accounting Office, Report to Agency Officials, Problems in Accounting for Navy Transactions Impair funds Control and Financial Reporting, GPO, Washington, DC, January 1999.

18. Department of Defense, Office of the Inspector General, Vendor Payments at Defense Accounting Offices, GPO, Washington, DC, 30 November 1995.

19. Defense Finance and Accounting Service, Accounting Systems Strategic Plan, [http://www.dfas.mil/library/dassp/plan3.htm]

20. Department of Defense, Under Secretary of Defense (Comptroller), Guide to Federal Requirements for Financial Management Systems, GPO, Washington, DC, August 1997.

21. Defense Finance and Accounting Services, DFAS Organization, [http://www.dfas.mil].

22. Department of Defense, Under Secretary of Defense (Comptroller), DoD Biennial Financial Management Improvement Plan, GPO, Washington, DC, October 1998.

23. Department of Defense, Office of the Inspector General, Vendor Payments-Operation Mongoose, GPO, Washington, DC, 30 May 1996.

24. United States Government Accounting Office, Department of Defense Status of Financial Management Weakness and Actions Needed to Correct Continuing Challenges GPO, Washington, DC, 4 May 1999.

25. United States Government Accounting Office, Major Management Challenges and Program Risks Department of Defense, GPO, Washington, DC, January 1999.

26. Defense Finance and Accounting Service, "Electronic Commerce," [http://www.dfas.mil/ecedi/edstar/]

27. Department of Defense, Under Secretary of Defense (Comptroller), Financial Management Reform, [http://www.dtic.mil/comptroller/index.html]

28. Fremgen, J. M., Introduction to Internal Control and Auditing, Naval Postgraduate School, Monterey, CA, August 1998.

29. Hleba, T., Financial Management in the Armed Forces, Naval Postgraduate School, Monterey, CA, September 1998.

30. Defense Finance and Accounting Service, STARS-FL Modification Training Course, Coopers and Lybrand Consulting, 1996.

31. Defense Manpower Data Center, Memorandum for Operation Mongoose-DFAS HQ/P, Subject: Congressional Report on Operation Mongoose (U), 5 January 1998.

32. Interview between Wright, L., GS-14, Operation Mongoose, Seaside, CA, and the author, 12 August 1999.

33. United States General Accounting Office, DoD Procurement Fraud, Fraud by an Air Force Contracting Official, GPO, Washington, DC, September 1998.

34. Stubbs, J. D., "Fighting Fraud Illustrated: The Robins AFB Case," The Air Force Law Review, 1994.

35. United States General Accounting Office, Financial Management: Improvements Needed in Air Force Vendor Payment Systems and Controls, GPO, Washington, DC, September 1998.

36. Telephone conversation between Major Bud Campbell, Air Force Office of Special Investigations and the author, 7 September 1999.

37. Wilson, G. C., “Senator: Fix DoD Fraud First, Then Ask For Money,” Navy Times, 12 October 1998.

38. Fox, H. J., Payroll Clerk Pleads Guilty to Embezzlement, [http://www.usdoj.gov/usao/gam/pr/gam60816.1.html], 16 August 1996.

39. Department of Defense, Headquarters, Air Force Office of Special Investigations, Semi-Annual Report on Fraud Operations, DPO, Fort Belvoir, VA, 12 March 1998.

40. Office of the Under Secretary of the Defense, (Comptroller), The Federal Financial Management Improvement Act, [http://www.dtic.mil/comptroller/fmfia]

41. The Financial Network, Improving Financial Management (Part 2), [www.financenet.gov/financenet/fed/cfo/gpca/aimd9852]

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center..2
8725 John J. Kingman Road, Ste 0944
Fort Belvoir, VA 22060-6218

2. Dudley Knox Library..2
Naval Postgraduate School
411 Dyer Road
Monterey, CA 93943-5101

3. Professor James M. Fremgen, Code SM/Fm...1
Naval Postgraduate School
Monterey, CA 93943-5103

4. Professor O. Douglas Moses, Code SM/Mo..1
Naval Postgraduate School
Monterey, CA 93943-5103

5. Operation Mangoose...1
400 Gigling road
Seaside, CA 93955-6771

6. Shawn Jones-Oxendine...2
912 Darren Drive
Portsmouth, VA 23701